Amendments to the Claims

1.   (Currently amended) A method for restricting use of a clipboard application, the method comprising:

        determining whether a copy selection associated with designated content of a source file being displayed by a first source application has been made;

        storing the designated content to the clipboard application; and

        determining whether the source file is a secured file, wherein the secured file includes a header having a file key available to an authenticated user, and wherein the secured file cannot be accessed without the file key; and

        ~~preventing subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is the secured file~~.

2.   (Previously presented) The method recited in claim 1, further comprising receiving a paste selection to provide the designated content to the second destination application.

3.   (Previously presented) The method recited in claim 2, wherein the paste selection requests to paste the designated content to a destination file that is opened within the second destination application.

4.   (Previously Presented) The method recited in claim 2, wherein the copy
selection is a copy command, and wherein the paste selection is a paste command.

5.   (Previously Presented) The method recited in claim 1, wherein the
determining operates to determine that the source file is the secured file based on security
information provided by the first source application.

6.   (Currently amended) The method recited in claim 5, wherein the
determining includes determining that the security information pertains to the source
document.

7-9.   (Canceled)

10.   (Currently amended) The method recited in claim [[1]]47, wherein the
preventing comprises:

         storing predetermined content to the clipboard application instead of the
     designated content in response to determining that the source file is the secured
     file.

11.   (Currently amended) The method recited in claim [[10]]47, wherein the
preventing comprises:

         storing the designated content to the clipboard application in response to
     determining that the source file is not the secured file.

12.   (Currently amended) The method recited in claim 11, further comprising:

receiving a paste selection to provide the designated content to the second

destination application;

~~supplying the predetermined content from the clipboard application to the~~

~~second destination application in response to the paste selection in response to~~

~~determining that the source file is the secured file; and~~

~~supplying the designated content from the clipboard application to the~~

~~second destination application in response to the paste selection in response to~~

~~determining that the source file is not the secured file~~.

13-15. (Canceled)

16.   (Currently amended) A method for restricting use of a clipboard

application, the method comprising:

receiving a copy selection associated with designated content of a source

file being displayed by a first source application; and

determining whether the source file is a secured file, wherein the secured

file includes a header having a file key available to an authenticated user, and

wherein the secured file cannot be accessed without the file key, wherein said

determining is performed by one or more computing devices; and

~~preventing subsequent storage of the designated content to a second~~

~~destination application via the clipboard application in response to determining~~

~~that the source file is the secured file~~.

17.   (Previously presented) The method recited in claim 16, further
comprising storing alternate content to the clipboard application in response to
determining that the source file is the secured file.

18.   (Previously Presented) The method recited in claim 17, wherein the
alternate content is one or more of blank content, predetermined content, or scrambled
content.

19.   (Currently amended) The method recited in claim 17, ~~wherein the~~
~~computer-implemented method~~ further ~~comprises~~ <u>comprising</u>:

~~permitting storage of the designated content to~~ <u>supplying the</u>

<u>predetermined content from</u> the clipboard application <u>to the second destination</u>

<u>application in response to the paste selection</u> in response to determining that the

source file is not the secured file.

20.   (Previously presented) The method recited in claim 16, wherein ~~the~~
~~computer-implemented method~~ further ~~comprises~~ <u>comprising</u>:

~~permitting storage of~~ <u>supplying</u> the designated content [[from]] <u>to</u> the

clipboard application ~~to the second destination application in response to the~~

~~paste selection~~ in response to ~~determining~~ that the source file is not the secured

file.

21.   (Previously Presented) The method recited in claim 20, wherein the

determining operates to determine that the source file is the secured file based on security

information provided by the first source application.

22.   (Currently amended) The method as recited in claim 21, wherein the

<u>determining includes determining that the</u> security information pertains to the source

document.

23 - 39.   (Canceled)

40.   (Currently amended) A tangible computer readable medium having

instructions stored thereon for restricting the use of a clipboard application, the

instructions comprising:

        instructions to receive a copy selection associated with designated content

        of a source file being displayed by a first source application;<u> and</u>

        instructions to determine whether the source file is a secured file, wherein

        the secured file includes a header having a file key available to an authenticated

        user, and wherein the secured file cannot be accessed without the file key~~, and~~

~~instructions to prevent subsequent usage of the designated content in a~~

~~second destination application via the clipboard application in response to~~

~~determining that the source file is the secured file~~.

41.   (Currently amended) The method recited in claim [[1]]51, wherein said
instructions to prevent comprise ~~preventing comprises~~:

            instructions to store ~~storing~~ blank content to the clipboard application in

     response to determining that the source file is a secured file.

42.   (Currently amended) The method recited in claim [[41]]51, wherein said
instructions to prevent comprise ~~preventing comprises~~:

            instructions to store ~~storing~~ the designated content to the clipboard

     application in response to determining that the source file is not a secured file.

43.   (Currently amended) The method recited in claim [[42]]41, wherein said
method further comprises:

            receiving a paste selection to provide the designated content to the second

     destination application;

            supplying the blank content from the clipboard application to the second

     destination application in response to the paste selection in response to

     determining that the source file is a secured file; and

supplying the designated content from the clipboard application to the

second destination application in response to the paste selection in response to

determining that the source file is not a secured file.

44.   (Currently amended) The method recited in claim [[1]]47, wherein said

preventing comprises:

storing scrambled content to the clipboard application in response to

determining that the source file is a secured file.

45.   (Currently amended) The method recited in claim [[44]]47, wherein said

preventing comprises:

storing the designated content to the clipboard application in response to

determining that the source file is not a secured file.

46.   (Previously presented) The method recited in claim 45, further

comprising:

receiving a paste selection to provide the designated content to the second

destination application;

supplying the scrambled content from the clipboard application to the

second destination application in response to the paste selection if said

determining determines that the source file is a secured file; and

supplying the designated content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not a secured file.

47.   (New) The method recited in claim 1, further comprising:

preventing subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is a secured file.

48.   (New) The method recited in claim 12, further comprising:

supplying the predetermined content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is a secured file.

49.   (New) The method recited in claim 12, further comprising:

supplying the designated content from the clipboard application to the second destination application in response to the paste selection in response to determining that the source file is not a secured file.

50.   (New) The method recited in claim 16, further comprising:

preventing subsequent storage of the designated content to a second destination application via the clipboard application in response to determining that the source file is the secured file.

        51.   (New)   The tangible computer readable medium of claim 40, the instructions further comprising:

        instructions to prevent subsequent usage of the designated content in a second destination application via the clipboard application in response to determining that the source file is a secured file.